

Abstract of the Disclosure

Let us consider a message M an element $(m1,m2, \dots, mk)$ in a Galois field $GF(2^k)$, and multiply it by a product of polynomials β $1(\alpha)$ - β $t(\alpha)$ into $M(\alpha)$.

$$M(\alpha) = M \beta 1(\alpha) \cdot M \beta 2(\alpha) \cdot \cdots \cdot M \beta t(\alpha)$$

Combine a noise vector $\mathbf{r}(\alpha)$ of \mathbf{n} - \mathbf{k} to $\mathbf{M}(\alpha)$ in series so that the data is expanded into degree \mathbf{n} . Next, they are transformed into Γ by permutation. Γ is multiplied by an element γ in the Galois field $\mathrm{GF}(2^n)$ into cyphertext $\mathrm{C}(\mathbf{M})$, where γ is a primitive root of the multiplicative group of the Galois field $\mathrm{GF}(2^n)$. Practically, when the message \mathbf{M} is substituted for \mathbf{X} in a public key $\mathrm{C}(\mathbf{X})$, the cyphertext $\mathrm{C}(\mathbf{M})$ is obtained. The cyphertext $\mathrm{C}(\mathbf{M})$ is multiplied by γ is applied to an inverse permutation, and the noise vector $\mathrm{r}(\alpha)$ is separated. Then, the inverse element of the product of β $1(\alpha) - \beta$ $1(\alpha)$ is multiplied and is raised to an adequate index. Then the decrypted message is obtained.